National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

JOINT FUSION INFORMATION FOR COMMAND AND CONTROL: PROPOSALS TO ENHANCE C4ISR INTEROPERABILITY IN THE CANADIAN ARMED FORCES

Lieutenant-Colonel Kareen Kate Montambault

JCSP 50

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 50

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 50 - PCEMI n° 50
2023 - 2024

Service Paper – Étude militaire

JOINT FUSION INFORMATION FOR COMMAND AND CONTROL: PROPOSALS TO ENHANCE C4ISR INTEROPERABILITY IN THE CANADIAN ARMED FORCES

Lieutenant-Colonel Kareen Kate Montambault

\

JOINT FUSION INFORMATION FOR COMMAND AND CONTROL: PROPOSALS TO ENHANCE C4ISR INTEROPERABILITY IN THE CANADIAN ARMED FORCES

AIM

1. The aim of this service paper is to address the absence of a joint interconnected Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) interface in the Canadian Armed Forces (CAF), which hampers the collection, processing, and dissemination of critical data in real-time. The intent is also to propose strategies to enhance joint interoperability within the CAF, specifically focusing on integrating sensors[1] and information across different domains and exploring potential approaches for the development of such a capability within the CAF.

INTRODUCTION

2. Effective joint interoperability is crucial in modern military operations, a fact recognized by the CAF in the Pan-Force Employment Concept (PFEC) and the Policy Strong Secure Engage (SSE). Despite these efforts, achieving joint capabilities remains challenging, especially in the rapidly evolving landscape of advanced technologies. A notable gap exists in the absence of a connected interface to enable a unified "pan-domain" picture, integrating legacy systems with emerging technologies like satellites, the Internet of Things (IoT), and Artificial Intelligence (AI) across various domains. This gap hampers seamless communication and coordination among military branches and with allies, impeding operational effectiveness.

3. The five main joint operational functions—Command, Act, Sense, Shield, and Sustain—are recognized as crucial for modern warfare, yet enabling them in a joint manner presents increasing difficulties. The fragmented nature of sensor and Command and Control systems across different CAF branches and agencies exacerbates this challenge, leading to inefficiencies and gaps in situational awareness. The paper will examine examples from Canada's allies, such as the North Atlantic Treaty Organization (NATO) and the US Department of Defense (DoD), showcasing global recognition of the importance of joint interfaces. Through these insights, the paper aims to offer a comprehensive understanding of the imperative and approach to achieving joint interoperability in CAF's C4ISR systems, referred to as Joint Fusion Information for Command and Control (JFI4C2) for the purpose of this work.

[1] In *Wikipedia,* a sensor is a device that produces an output signal for the purpose of sensing a physical phenomenon. In the broadest definition, a sensor is a device, module, machine, or subsystem that detects events or changes in its environment and sends the information to other electronics, frequently a computer processor. https://en.wikipedia.org/w/index.php?title=Sensor&oldid=1200677558.

DISCUSSION

4. The lack of a unified interface within the CAF poses complex challenges that hinder efficient joint interoperability. The root of these challenges stems from the fragmented systems dispersed among various elements, platforms and organizations within the CAF. Each operates its own set of sensors, often with disparate technologies, standards, and formats. Consequently, there is no standardized approach for collecting, processing, and sharing sensor data, leading to inefficiencies, redundancies, and gaps in situational awareness.

5. For instance, various entities utilize systems such as the Blue Force Tracker for tracking friendly forces, while the Air Force employs Link 16 and 22 to facilitate picture and live video feeds of the situation. Additionally, radar squadrons and Air Traffic Control (ATC) utilize CRC System Interface (CSI), and the Navy has recently adopted drones for exercising targets (Unmanned Surface Vehicles and Unmanned Aerial Vehicles), as well as for enabling ISR operations of areas Beyond Line-Of-Sight (BLOS) utilizing systems like WinTAK.

6. Very recently, the North American Aerospace Defense Command (NORAD) organization tested the new cloud-based Command and Control (CBC2) system in North Bay. This system integrates a wide array of tactically relevant data feeds alongside AI and machine learning capabilities to enable decision-makers to maintain a comprehensive situational awareness of the environment.[2]

7. Additionally, the Assistant Deputy Minister – Chief Information Officer (ADM(CIO)) has launched the Network Command and Control Integrated Situational Awareness Capability (Net C2 ISAC) project, with a budget of $50 to $99 million.[3] Developed by General Dynamics Mission Systems Canada and CDW Canada, this solution aims to provide real-time monitoring of critical Information Technology (IT) services, enhance cyber resilience, and utilize AI for optimized decision-making.[4] While empowering commanders with comprehensive IT service information, it falls short of serving as a joint interface for warfare operations.

8. Lieutenant-General Paul, Commander of the Canadian Army (CA), recently announced a $1.68 billion project named the Land C4ISR (LC4ISR) system in December 2023.[5] This initiative aims to enhance the LC4ISR capability by establishing a

---

[2] Maxime Cliche, "Canadian Air Defence Sector Introduces New Cloud-Based Command-and-Control System," *North American Aerospace Defense Command*, 2024, https://www.norad.mil/Newsroom/Article/3657967/canadian-air-defence-sector-introduces-new-cloud-based-command-and-control-syst/.

[3] Canada, Department of National Defence, "Network Command Control Integrated Situation Awareness Capability - Defence Capabilities Blueprint," 2018, https://apps.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=960.

[4] Department of National Defence, "Network Command Control Integrated Situation Awareness Capability - Defence Capabilities Blueprint."

[5] Canada, Public Services and Procurement, "Canada Announces $1.68-Billion Investment in Technology Network for Canadian Army," news releases, 2023.

consolidated, secure network of tactical communications systems tailored specifically for land operations. It is important to note that although this capability aims to serve in an operational environment, it is designed for land operations and does not specifically encompass joint operations.

9. These are just a few examples, acknowledging that the military utilizes numerous data feeds that often operate independently without seamless communication. As a result, operation centers are becoming increasingly crowded, with multiple screens displaying diverse information, sometimes limited to raw data. This situation demands operators to swiftly analyze this multitude of data to ensure timely and accurate decision-making. The scattered nature of information leads to confusion, making it challenging to attain a comprehensive and timely common operational picture.

10. One of the main reasons for this fragmented approach is the structure within the Department of National Defence (DND), which primarily facilitates Force Development (FD) through silos. Each element operates independently, allocating funds based on its own requirements. Despite growing recognition of the need for joint forces and enhanced intercommunication capabilities, there is no designated organization mandated to develop joint operational capabilities. While the Canadian Joint Operations Command (CJOC) advocates for pan-domain operations, its authority is limited to Force Employment (FE) exclusively. As illustrated in Figure 1, the PFEC primarily focuses on operational strategies for FE entities.[6] While institutional initiatives may discuss pan-domain intentions, there is no clear mandate for FD to adopt a joint mindset for future force employment. Consequently, the question arises: which organization should be responsible for developing essential joint capabilities?

Figure 1 – Defence Strategy Map adapted from SJS
Source: PFEC

11. Canadian Special Operations Forces Command (CANSOFCOM) stands out as the sole domain encompassing all five functional domains (5 "F"): FE and FD (mentioned

[6] Canada. Department of National Defence. "Pan-Domain Force Employment Concept: Prevailing in an Uncertain World" (Ottawa: CJOC, 2023), 13.338.47355 E26 2020 CFC

earlier), Force Generation (FG), Force Sustainment (FS) and Force Management (FM). It is the only organization truly proficient in pan-domain operations, expertly planning and coordinating across the three conventional elements—land, air, and sea. Additionally, CANSOFCOM seamlessly integrates the emerging domains of cyber and space and collaborates with both allies and other government agencies. While the rest of the CAF have much to glean from their operational approach, particularly in FD, procurement processes, and equipment compatibility, it is essential to note that CANSOFCOM cannot singularly shoulder the responsibility for developing and sustaining a joint force across all domains and services.

12. While ADM(CIO) is considered a "purple" organization, historically it has primarily focused on providing institutional support rather than directly addressing operational functions. Operational aspects have traditionally fallen under the purview of CANSOFCOM, CJOC and its FG units. However, in recent years, ADM(CIO) has expanded its mandate to encompass operational domains, albeit encountering inherent complexities along the way. This expansion includes navigating responsibilities within cyber operations and managing space support through communication contracts for operational purposes. Additionally, it oversees the deployment of level III capabilities in theatre. Thus, ADM(CIO) emerges as a potential candidate to take on the responsibility of developing the new operational joint capability.

13. Another compelling argument for the CAF to establish a JFI4C2 capability is the imperative to adapt to the rapidly evolving environment of modern warfare. The utilization of advanced military technologies in conflicts such as the ongoing Russia-Ukraine war underscores the necessity for continuous technological advancements within NATO. As articulated by the article by Budning, *et al,* "A Connected Battlefield would help Canada prepare for a new generation of threats and operations stemming from the return of great power (and data-driven) competition between the US, China, and Russia".[7] This interconnectedness across domains of warfare is crucial for synchronizing effects, thereby enhancing military capabilities, deterring adversaries, and improving freedom of action.[8] To further underscore the significance of this initiative, several countries have already commenced similar projects.

14. NATO has recently introduced the Joint Information Surveillance and Reconnaissance (JISR) system. This system amalgamates data and information gathered from various sources, including NATO's Alliance Ground Surveillance (AGS) system and Airborne Warning & Control System (AWACS) surveillance aircraft, alongside national JISR assets spanning space, air, land, and maritime domains. Surveillance and reconnaissance operations encompass both visual observation, such as ground soldiers, and electronic observation from satellites, unmanned aircraft systems, ground sensors, and maritime vessels. These inputs are subsequently analyzed to transform raw data into

[7] Kevin Budning, Alex Wilner, and Guillaume Cote, "Connecting the Dots on Canada's Connected Battlespace," *International Journal*, no. 76(1) (2021): 2.
[8] Ibid.

actionable intelligence.[9] NATO Allies endorsed a new strategy in October 2020, guiding the development and deployment of interoperable intelligence capabilities in a more agile manner. This strategy leverages cutting-edge technologies like big data, AI, and autonomous systems to enhance NATO's intelligence-gathering capabilities.

15. While the UK, France, and Germany have initiated similar projects and formulated recent strategies,[10] Canada can look closer to home for another example. The US DoD is actively involved in developing this type of capability. They have formulated a joint doctrine that informs and considers multinational and allied joint doctrines to enhance interoperability in future competition and conflict.[11] In 2022, the DoD released the joint all-domain Command and Control (JADC2) Strategy and Implementation Plan. The JADC2 aims to integrate and synchronize military operations across all domains (land, air, sea, space, and cyberspace), linking sensor data to command centers to enable rapid response across various military branches, agencies, and allies. The strategy leverages advanced technologies, such as AI, machine learning, and networked sensors, to provide commanders with real-time situational awareness and the ability to respond to evolving threats rapidly. JADC2 is designed to ensure interoperability, resilience, and agility in multi-domain operations, ultimately enhancing the US military's ability to deter adversaries and achieve strategic objectives.[12] In military terms, "JADC2 enables the Joint Force to *sense, make sense*, and *act* on information across the battlespace".[13] The implementation plan provides plans, resources, and milestones to reach the endpoint, and while this might seem more like a philosophy at this moment, someone is taking responsibility, and the DoD has a strategy it can build on, as depicted by JADC2 placemat (see figure 2).

[9] NATO, "Joint Intelligence, Surveillance and Reconnaissance," NATO, 2023, https://www.nato.int/cps/en/natohq/topics_111830.htm.
[10] Simona R. Soare, Pavneet Singh, and Meia Nouwens, "Software-Defined Defence: Algorithms at War," 2023, https://policycommons.net/artifacts/3453438/software-defined-defence/4253736/.
[11] Department of Defense United States, "Implementing Joint Force Development and Design" (Joint Staff; Washington, 2022).
[12] Department of Defense United States, "Summary of the Joint All Domain Command and Control Strategy," 2022.
[13] Sean Carberry, "Joint All-Domain Command, Control A Journey, Not a Destination," *National Defense Industrial Association Business & Technology Magazine*, Defense Department's joint all-domain command and control, 2023, https://www.nationaldefensemagazine.org/articles/2023/7/10/joint-all-domain-command-control-a-journey-not-a-destination.

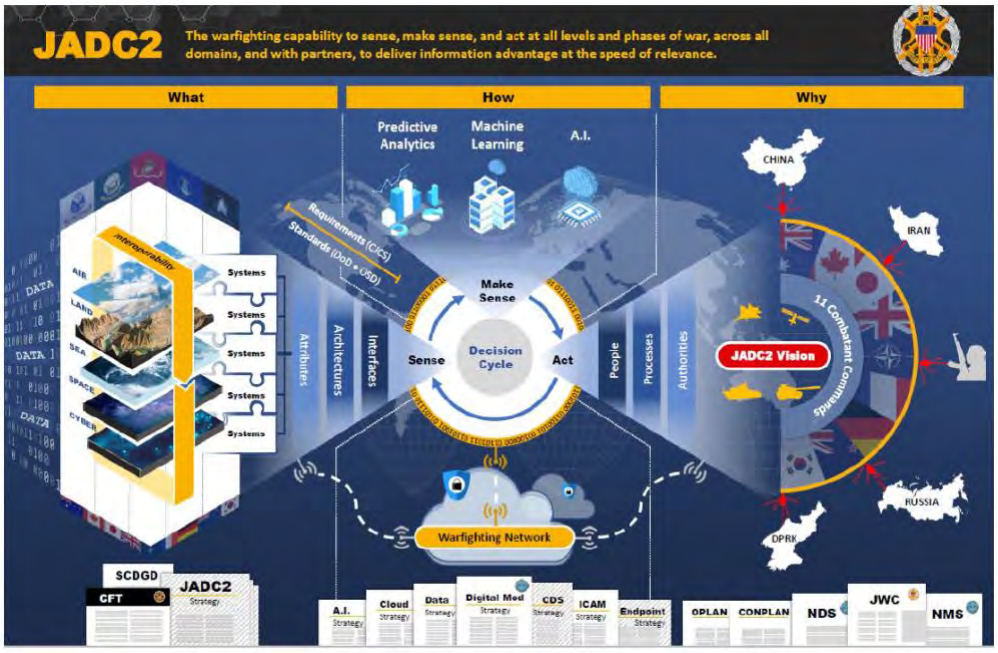

Figure 1 JADC2 Placemat

Figure 2. JADC2 Placemat

Source: Summary of the Joint All Domain Command and Control Strategy

16. Additionally, DoD is focusing on a new cloud service called the Joint Warfighter Cloud Capability (JSCC) to support its strategy. This initiative replaces the cancelled Joint Enterprise Defense Infrastructure (JEDI) cloud.[14] Also, similar to the PFEC, the DoD developed the Joint Warfighting Concept (JWC), which guides the development efforts of each service in the American military, emphasizing connectivity and synchronization of joint capabilities. With seven key tenets, it underscores the need for a system enabling joint coordination and rapid decision-making.[15] With the JEDI, its JWC, JADC2 Strategy, and implementation, it is evident that the DoD prioritizes jointness and recognizes the necessity of a joint interface.

17. There is a pressing need to prioritize the development of this capability from a coalition perspective. Members of the Five Eyes, NATO, and NORAD are actively engaged in crafting doctrine, conceptualizing strategies, and formulating implementation plans for a joint all-domain interface capability. Without undertaking an initiative of this magnitude, Canada risks hindering its capacity to integrate both new and existing systems with our allies seamlessly. This potential shortfall could lead to fractures in crucial relationships and undermine trust within major coalitions, thereby diminishing Canada's ability to offer substantive contributions to allied decision-making processes.[16] Once again, the reputation of Canada and its military prowess hangs in the balance with our

[14] United States. Department of Defense. "Future of the Joint Enterprise Defense Infrastructure Cloud Contract." (2021) https://www.defense.gov/News/Releases/Release/Article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/

[15] Thomas A. Walsh and Alexandra L. Huber, "A Symphony of Capabilities How the Joint Warfighting Concept Guides Service Force Design and Development," *Joint Force Quarterly : JFQ*, no. 111 (2023): 4–15.

[16] Budning, Wilner, and Cote, "Connecting the Dots on Canada's Connected Battlespace."

allies and partners. It's worth noting that Canada's defence industry most likely possesses the requisite expertise and capabilities to develop such an interface.[17] Therefore, the DND should capitalize on the strengths of its defence industry to position itself not merely as a consumer but rather as a global leader and contributor to allied military innovation.

CONCLUSION

18. In conclusion, developing a JFI4C2, especially in the context of multi-domain operations, is of paramount importance. The urgent need for the CAF to establish a joint interface capable of aggregating diverse sensor data and fostering interoperability cannot be overstated. The fragmented nature of sensor systems across different branches, elements and organizations within the CAF presents significant challenges, including inefficiencies, redundancies, and gaps in situational awareness, hindering timely decision-making and response to threats. Additionally, the rapid evolution of modern warfare and the resurgence of great power competition emphasize the urgency for Canada to enhance its military capabilities. Examples such as initiatives by NATO and the US DoD underscore the global recognition of the importance of joint interfaces. Failure to address this capability gap not only hampers Canada's ability to integrate with allies and contribute to coalition efforts but also risks undermining trust and credibility within key partnerships.

19. To achieve even deeper integration and enhance the common operating picture, it is worthwhile considering the potential benefits of incorporating additional sensors and improving connectivity with all end-users, including soldiers and various vehicles. Currently, relying solely on IoT devices and satellites may be premature for the CAF. It's essential to adopt a gradual approach, learning to walk before running. Leveraging CAF end-users for the initial phase and ensuring that sensor feeds are connected or compatible with a unified interface could prove more effective in the early stages. Therefore, further analysis would be valuable to investigate the feasibility of integrating sensors into our end-user equipment and determining optimal deployment locations.

RECOMMENDATIONS

20. The following recommendations outline key steps for addressing the critical capability gap in joint connected interface systems and developing a JFI4C2 within the CAF:

a. Formulate a comprehensive joint strategy to enhance C4ISR systems interoperability across all branches and agencies within the CAF.

b. Establish collaborative initiatives with allied nations to advance joint interface capabilities and interoperability in C4ISR systems, while fostering interagency and industry partnerships to support joint solutions development and implementation.

[17] Christyn Cianfarani, "Getting Canada to a Wartime Footing: Clear Parameters Are Required," *Canadian Global Affairs Institute*, 2023, https://www.cgai.ca/getting_canada_to_a_wartime_footing.

c. Designate a specific organization within the CAF to serve as the focal point for joint force development in C4ISR, tasked with coordinating efforts, setting priorities, and driving forward the implementation of joint interface capabilities.

d. Investigate the potential of embedding sensors directly at the end-user level to bolster situational awareness and bolster connectivity within C4ISR systems.

BIBLIOGRAPHY

Budning, Kevin, Alex Wilner, and Guillaume Cote. “Connecting the Dots on Canada’s Connected Battlespace.” *International Journal*, no. 76(1) (2021): 154–62.

Carberry, Sean. “Joint All-Domain Command, Control A Journey, Not a Destination.” *National Defense Industrial Association Business & Technology Magazine*, Defense Department’s joint all-domain command and control, 2023. https://www.nationaldefensemagazine.org/articles/2023/7/10/joint-all-domain-command-control-a-journey-not-a-destination.

Cianfarani, Christyn. “Getting Canada to a Wartime Footing: Clear Parameters Are Required.” *Canadian Global Affairs Institute*, 2023. https://www.cgai.ca/getting_canada_to_a_wartime_footing.

Cliche, Maxime. “Canadian Air Defence Sector Introduces New Cloud-Based Command-and-Control System.” *North American Aerospace Defense Command*, 2024. https://www.norad.mil/Newsroom/Article/3657967/canadian-air-defence-sector-introduces-new-cloud-based-command-and-control-syst/.

Department of National Defence. “Network Command Control Integrated Situation Awareness Capability - Defence Capabilities Blueprint,” 2018. https://apps.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=960.

Canada. Department of National Defence. “Pan-Domain Force Employment Concept: Prevailing in an Uncertain World.” Ottawa: CJOC, 2023.

NATO. “Joint Intelligence, Surveillance and Reconnaissance.” NATO, 2023. https://www.nato.int/cps/en/natohq/topics_111830.htm.

Public Services and Procurement, Canada. “Canada Announces $1.68-Billion Investment in Technology Network for Canadian Army.” News releases, 2023. https://www.canada.ca/en/public-services-procurement/news/2023/12/canada-announces-168-billion-investment-in-technology-network-for-canadian-army.html.

“Sensor.” In *Wikipedia*, January 30, 2024. https://en.wikipedia.org/w/index.php?title=Sensor&oldid=1200677558.

Soare, Simona R., Pavneet Singh, and Meia Nouwens. “Software-Defined Defence: Algorithms at War,” 2023. https://policycommons.net/artifacts/3453438/software-defined-defence/4253736/.

United States. Department of Defense. “Future of the Joint Enterprise Defense Infrastructure Cloud Contract.” In *U.S. Department of Defense*. Pentagon; Washington: U.S Department of Defense, 2021. https://www.defense.gov/News/Releases/Release/Article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/

United States. Department of Defense. “Implementing Joint Force Development and Design.” Joint Staff; Washington, 2022. https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203030.01A.pdf

United States. Department of Defense. “Summary of the Joint All Domain Command and Control Strategy.” 2022. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

Walsh, Thomas A., and Alexandra L. Huber. “A Symphony of Capabilities How the Joint Warfighting Concept Guides Service Force Design and Development.” *Joint Force Quarterly : JFQ*, no. 111 (2023): 4–15. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3568312/a-symphony-of-capabilities-how-the-joint-warfighting-concept-guides-service-for/